Supply Chain Cyber-Resilience: Creating an Agenda for Future Research

Khan, Omera; Sepúlveda Estay, Daniel Alberto

Published in:
Technology Innovation Management Review

Publication date:
2015

Document Version
Publisher's PDF, also known as Version of record

Supply Chain Cyber-Resilience: Creating an Agenda for Future Research

Omera Khan and Daniel A. Sepúlveda Estay

> *"Resilience is all about being able to overcome the unexpected. Sustainability is about survival. The goal of resilience is to thrive."*
>
> Jamais Cascio
> Writer and futurist specializing in design strategies

Supply chains have become more vulnerable in recent years, and high-profile cyber-attacks that have crippled the supply chains of well-known companies reveal that the point of entry for hackers is often through the weakest link in the chain. Exacerbated by growing complexity and the need to be visible, these supply chains share vital streams of information every minute of the day, thereby becoming an easy and highly lucrative target for talented criminals, causing financial losses as well as damaging brand reputation and value. Companies must therefore invest in supply chain capabilities to withstand cyber-attacks (i.e., cyber-resilience) in order to guard against potential threats. They must also embrace the reality that this often-unknown dimension of risk is the "new normal". Although interest on this topic has grown in the business world, less has been reported by the academic community. One reason for this could be due to the convergence of two different disciplines, information technology and supply chains, where supply chain cyber-risk and cyber-resilience appear to have a natural fit. The topic of cyber-resilience in supply chains is still in early stages of development, and this is one of the first journals to focus a special issue on it. Currently, the closest academic literature is within the realms of supply chain risk and resilience, where numerous models and frameworks exist. In this article, this literature is explored to identify whether these models can incorporate the dimension of cyber-risk and cyber-resilience. In doing so, we create a research agenda for supply chain cyber-resilience and provide recommendations for both academia and practice.

Introduction

Supply chain management has become dependent on electronic systems; since the 2000s, we have seen the emergence of information technology solutions to support business operations, to share information, to connect businesses, and to generate greater visibility along supply chains in order to gain knowledge and control of processes. On the other hand, although supply chains have pursued aspects such as the standardization of business processes, increased communication, connectivity, and data exchange, the vulnerability of these systems to cyber-attacks is nevertheless increasing. Why is this? In modern supply chains, information is shared digitally more than any other way, and supply chains are so reliant on good quality information that, without it, supply chain managers cannot make decisions on forecasts, production, distribution, etc. Equally importantly, poor data leads to poor decisions and performance. So, even with the most efficient and responsive supply chain, performance will be greatly compromised without good quality information.

For supply chains to thrive, managers must recognize that cyber-attacks are becoming common occurrences and that the "new normal" operating environment is one that is increasingly impacted by unknown risks. A key lesson for supply chain managers is that cyber-attacks do not always "come through the front door"; a business can be greatly impacted by an attack on the weakest link in their supply chain. A key difficulty with cyber-attacks is that often a business will not know the

Supply Chain Cyber-Resilience: Creating an Agenda for Future Research

Omera Khan and Daniel A. Sepúlveda Estay

types of cyber-risks to which it has exposure, until it realizes that it is being attacked. Therefore, businesses must develop cyber-resilience to protect their supply chains.

Cyber-attacks can cause considerable economic costs to the companies that suffer these breaches, although the costs may not be noticed until after the damage is done. Estimates of the annual costs from cyber-crimes range from $375 billion to $575 billion (USD) (Intel Security, 2014), with significant effects on supply chains and resulting business performance with customers. Missing or erroneous data and information in supply chains, as a result of cyber-attacks, can lead to undesirable effects as diverse as intellectual property breaches, sub-standard or interrupted operations, sensitive data custody breaches, and decreases in service level to final customers. For example, some estimates indicate annual losses of £9.2bn from the theft of intellectual property and a further £7.6bn from industrial espionage.

Businesses that are able to understand what data is critical, where it is, who has access to it, and who is responsible for it, as well as where potential risks are in terms of information and data in the supply chain, are those that will be able to correctly communicate these risks to the supply chain in order to implement actions to mitigate them.

However, there has been a lack of managerial action to acknowledge the relevance and impact of cyber-crime (Burnson, 2013; Deloitte, 2012, 2013). It has been stated that "only a few CEOs realize that the real cost of cyber-crime stems from delayed or lost technological innovation" (Bailey et al., 2014) and companies have likely underestimated their risk (Intel Security, 2014). This is, either by delayed decision making or by a lack of awareness, the resulting inaction is leading to higher organizational costs from cyber-crimes.

This inaction is compounded by the increasing complexity of global supply chains and the speed and connectivity of operations required by companies to stay competitive. Furthermore, the growing skill of the attackers to find novel ways of accessing crucial data (Reuters, 2012), and the limited information and tools available to manage these threats, requires organizations to be more resilient to cyber-attacks that can cripple their supply chains.

Companies can prepare for potential attacks by applying appropriate supply chain risk-management tools and techniques both to reduce the likelihood of an intrusion and to deal with any disruption should an attack be successful. Every business that depends on a supply chain needs to build in cyber-resilience. But what exactly is cyber-resilience in the context of supply chains, and how can it be incorporated into current supply chain risk-management approaches?

Cyber-risk has been defined by the Institute for Risk Management (IRM, 2015) as "any risk of financial loss, disruption or damage to the reputation of an organization from some sort of failure of its information technology systems". The ISO 27005:2008 defines information security risk as "the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization" (BSI, 2008). Both of these terms are being widely used in industry, and this article will consider these terms as equivalent.

We define supply chain cyber-resilience "as the capability of a supply chain to maintain its operational performance when faced with cyber-risk".

In light of the above challenges, the purpose of this article is to create an agenda for future research that could help supply chain and IT personnel to recognize and take a proactive team-based approach to supply chain cyber-resilience. More specifically, the aims of this study are to:

1. Explore current supply chain risk and resilience frameworks

2. Analyze these frameworks and determine whether they incorporate cyber-risk

3. Create a research agenda for cyber-risk and cyber-resilience.

The remainder of this article is structured as follows. First, the process used to find and review the key literature is explained. Next, the main findings of the literature review are discussed. Finally, a research agenda for supply chain cyber-resilience is proposed, including recommendations for both academia and industry.

Methodology

A systematic literature review was conducted, based on documented guidelines (Tranfield et al., 2003) through which a comprehensive, explicit, and reproducible method is followed. This method consists of ten steps that can be grouped into five main phases:

Supply Chain Cyber-Resilience: Creating an Agenda for Future Research

Omera Khan and Daniel A. Sepúlveda Estay

1. **Planning:** The planning phase focused on defining a review question to guide the search: "Do the current supply chain risk and resilience frameworks incorporate cyber-risk?"

2. **Searching:** The searching phase was guided by the identification of the relevant databases where the search was to be done, the keywords to be used during these searches, and the appropriate timeframe for the resulting documents to be included in the research. We searched for literature using the following databases: Scopus, Web of Science, ProQuest, and Google Scholar. The search keywords were determined from a knowledge domain analysis around the concept of cyber-resilience for the supply chain (see Figure 1). The three main knowledge domains to be scanned were identified as "supply chain management", "information technology management", and "risk (& resilience) management".

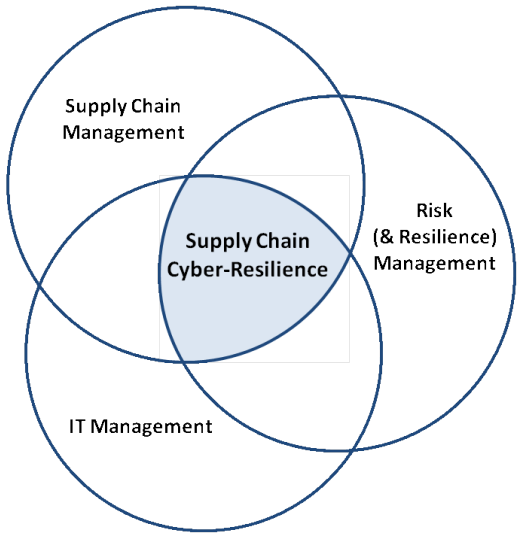

Figure 1. Main knowledge domains in supply chain cyber-risk management

3. **Screening:** After the initial, broad literature search was carried out, we conducted a preliminary analysis of the document titles and abstracts, if available. This step was followed by a more detailed analysis of the document abstracts, in the case of papers, and extended content in other cases. We applied explicit inclusion and exclusion criteria (e.g., document type, themes covered, research approaches) to identify a refined selection of documents for this analysis. Finally, the references of this refined set of articles were reviewed to identify relevant documents that might not have been identified through our initial broad search. Our final list consisted of 213 documents (24 articles, 137 peer-reviewed journal papers, 51 reports by specialized agencies, and 1 thesis). The documents covered the areas of supply chain risk management (131 documents), supply chain cyber-risk management (SCCRM), and information technology risk management (44 documents), ranging from the years 1998 to 2015.

4. **Extracting and synthesizing:** The documents were analyzed and synthesized using a spreadsheet format that allowed us to categorize the documents according to methodological approaches, contexts, outcomes, etc.

5. **Reporting:** In the next section, we report on our findings from the literature review.

Findings

Some of the earliest evidence of supply chain resilience can be found in the work of Christopher and Peck (2004), which was derived from earlier research on supply chain agility as a way of counteracting for uncertainty in the demand (Christopher & Towill, 2001), This perspective emerged after the foot-and-mouth disease event in the United Kingdom and the 9/11 terrorist attacks in United States, both of which occurred in 2001. Christopher and Peck proposed a reference model for the characterization of resilience in the supply chain, and the main aspects contributing to supply chain resilience were identified as re-engineering, organizational culture, agility, and collaboration.

Sheffi and Rice (2005) presented a disruption model based a proposed disruption theory for production systems (Asbjornslett, 1999), where this model was represented as a transient decrease in process performance. The Sheffi and Rice model identified eight sequential phases describing a disruption event: preparation, disruptive event, first response, initial impact, time of full impact, preparation for recovery, recovery, and long-term impact. Based on this model, Sheffi and Rice propose an enterprise "vulnerability map" through which the different disruption event probabilities and consequences are compared and ranked for prioritization.

Sheffi and Rice (2005) also identified product demand as the main source of uncertainty in the supply chain and acknowledged the increase in global uncertainty due to increased customer expectations, more global competition, longer and more complex supply chains, greater product variety, and shorter product lifecycles.

Supply Chain Cyber-Resilience: Creating an Agenda for Future Research

Omera Khan and Daniel A. Sepúlveda Estay

They considered organizational resilience as a strategic initiative to reduce vulnerability and therefore reduce the likelihood of occurrence of a disruption. Finally, they identified three important factors for building resiliency in an organization: redundancy, flexibility, and cultural change.

A number of other resilience frameworks have been suggested in literature. Linkov and colleagues (2013) proposed a resilience matrix of four steps representing a process for the event management cycles of disruptions: i) plan/prepare, ii) absorb, iii) recover, and iv) adapt. Each of these steps are described for different domains within the organization (i.e., physical, information, cognitive, and social). These authors have further suggested how to measure resilience according to this matrix.

Based on the framework proposed by Christopher and Peck (2004) as well as an empirical research study to identify vulnerabilities and capabilities within organizations, Pettit, Fiskel, and Croxton (2010) proposed the supply chain resiliency assessment and management (SCRAM) framework. This framework identifies an active relationship between the capabilities and the vulnerabilities in an organization, and its resulting resilience. They argue that the level of resilience that a company has to aim for is a balance between developing too many vulnerabilities (due to a lack of investment in capabilities), which could result in disruptions with undesirable economic effects, and investing in too many capabilities, which would erode profitability. Hence, they highlight an economic tradeoff between investment (capabilities) and risk (vulnerabilities).

Blackhurst, Dunn, and Craighead (2011) proposed a global resiliency framework based on systems theory and the framework proposed by Sheffi and Rice (2005). They distinguish between "resilience enhancers" and "resilience reducers", which are organizational attributes that either increase or decrease the ability of a firm to recover quickly and efficiently from a disruptive event. They identified 13 resilience enhancers and seven resilience reducers, each within three categories. Their work derives these attributes from an industrial setting and therefore can serve as basis for further research in the empirical confirmation of these or other resilience attributes.

The World Economic Forum (WEF, 2013) presented a resilience framework as part of its Supply Chain Risk Initiative. This framework attempts to quantify the risk to an organization's physical and intangible assets through a combination of effects from the existing risks to the organization and its vulnerabilities. The World Economic Forum's (WEF, 2013) resilience report also provides four recommendations for organizations to build resilient supply chains: i) put in place strong policies for the creation and adoption of resilience standards; ii) develop agile and adaptable strategies in organizations; iii) use data-sharing platforms for risk identification and response; and iv) enter into partnerships that involve all stakeholders in the risk assessment process.

Cyber-risks within the supply chain resilience framework

Our literature review did not find any supply chain resilience framework that incorporated the phenomenon of cyber-risk or information risk explicitly. However, our analysis revealed that the most influential sources for the development of cyber-resilience policy are the insurance industry, governmental requirements, and international organizations such as the World Economic Forum.

In 2012, the World Economic Forum created an initiative called "Partnering for Cyber-Resilience", led by Elena Kvochko, as a response to the increasing importance of cybersecurity. With more than 100 organizations involved, this initiative has created a series of reports describing principles for cybersecurity, recognizing interdependence, leadership, integrated risk management, and uptake by partners in the supply chain, as crucial aspects for resilience building. Additionally Kvochko has recently published an initial framework for the measurement of cyber-threats, through the calculation of a cyber-risk value and by combining eight factors grouped in three categories: vulnerability, assets, and attacker profile (WEF, 2015).

At a government level, there are several initiatives in place concerning cyber-risk and cybersecurity. In 2003, the United States government published the "National Strategy to Secure Cyberspace" (White House, 2003), and as part of a wider strategy from the Department of Homeland Security as a response to the 9/11 terrorist attacks and in line with Presidential Directive 63, which provides a framework for the protection of critical infrastructure (White House, 1998). In 2005, Germany started the "National Plan for Information Infrastructure Protection", with its main objectives being prevention, preparedness, and sustainability of the information infrastructure through the setting of international standards (German Federal Ministry of the Interior, 2005). By 2015, all EU member states except Portugal had published national cybersecurity strategies, with Estonia

Supply Chain Cyber-Resilience: Creating an Agenda for Future Research

Omera Khan and Daniel A. Sepúlveda Estay

having been the first in 2008 (ENISA, 2015; Keegan, 2014). In 2013, the United States government released Presidential Policy 21 and Executive Order 13636 to focus national attention on cyber-infrastructure resilience. In particular, Executive Order 13636 establishes a risk-based standard to protect critical infrastructure against cyber-threats. However, standards based on risk assessment do not necessarily create resilience (Linkov et al., 2013).

Conclusions and Recommendations

Our systematic literature review highlights that there is limited literature and no specific frameworks for cyber resilience in the supply chain, despite the increasing importance of the topic. The main supply chain resilience theories were proposed in the early 2000s, and the main advancements to those theories have been through the empirical identification of organizational attributes that increase or decrease resilience, as well as theoretical relationships between organizational vulnerabilities and capabilities as related to resilience. Additionally, we found that the existing supply chain resilience frameworks could be extended to consider cyber-risks through aspects such as cultural change (Sheffi & Rice, 2005) or collaboration and organizational culture (Christopher & Peck, 2004). Cyber resilience theory can also be advanced through the empirical quantification of the cyber-resilience of an organization, through case studies and stress testing of organizations with techniques such as non-invasive games (Gerencser et al., 2003).

A key contribution of this article is a definition for supply chain cyber-resilience: "the capability of a supply chain to maintain its operational performance when faced with cyber-risk". Furthermore, as a result of this study, we offer the following recommendations for academia with the goal of developing a future research agenda for supply chain cyber-resilience:

1. **Develop theory to demystify cyber-risk and cyber-resilience in supply chains:** Academics should conduct in-depth (systematic) literature reviews that confirm or expand on this study to devise methods of incorporating cyber-resilience with existing frameworks in supply chain resilience and indeed develop new models and frameworks. Finally, and fundamentally, they should align supply chain thinking and personnel with information technology issues and personnel to develop a team approach to supply chain cyber-resilience.
2. **Develop applicable tools and techniques:** There is a need for models (e.g., models of dynamic behaviour, machine-learning models for real-time monitoring of performance conditions) and practitioner workbooks (e.g., to evaluate the likelihood of detection or the probability of attack), to help practitioners better manage the causes and effects of cyber-risk to the supply chain.
3. **Generate case studies:** In-depth and longitudinal case studies within different industrial sectors are required to increase our understanding of the occurrence, detection, and reaction to cyber-attacks. Such case studies will enable researchers to validate theory and conceptual frameworks and models.
4. **Investigate the different types of cyber-attacks:** Studies should examine the attack goals (e.g., data theft, data modification, data falsification), the technical nature of attacks (e.g., tools, physical or digital barriers, verification procedures, data integrity), as well as human dimensions (e.g., cyber-attacker motivation, incentives).
5. **Propose strategic ways of managing cyber risks:** For example, academia may suggest portfolio investment to hedge risk by diversifying the business structure, where different areas counterbalance the effect of cyber-attacks. Furthermore, academia may suggest establishing appropriate key performance indicators or reviewing organizational culture and leadership, which should be empowered for proactive management of supply chain cyber-resilience.

For industry, we offer the following recommendations:

1. **The search for solutions to cyber-risks must be approached in terms of distributed accountability, instead of centralized authority:** The increasingly complex supply arrangements are creating conditions for "malevolent actors to recruit, coordinate and inflict harm across the whole network" (WEF, 2012). This challenge will require companies to adjust the current paradigm of centrally controlling risk management with routine evaluation processes (Deloitte, 2012).
2. **Re-arrange resources and develop contingency plans when necessary:** Organizations that thrive are those that can quickly recognize unusual operating conditions. It is no longer possible to prepare for every possible threat scenario. Instead, organizations

Supply Chain Cyber-Resilience: Creating an Agenda for Future Research

Omera Khan and Daniel A. Sepúlveda Estay

should prepare by encouraging team members to speak up when they detect an anomaly, having strategies in place to create customized contingency plans as necessary, and using automatic detection systems (e.g., machine learning) to identify real-time suspicious variations in performance indicators. There is a need for a new level of coordination in organizations for risk management and security response. In environments with high volatility, central controls are not sufficient and "structural integration is key to addressing uncertainties" (Boyson, 2014).

3. **Include recovery costs in the cost evaluation of cyber-attacks:** Recovery costs can surpass the direct organizational losses from cyber-attacks (Ponemon, 2014). Including recovery costs in the evaluations will highlight the real economic implications of delayed action.

4. **Create a cyber-crisis team within each organization:** Such teams should be empowered to work across organizational silos.

5. **Collaborate with academic institutions:** Academics can assist companies through training programs in cyber-resilience, by introducing new tools for the evaluation of cyber-resilience, or by providing methods for the real-time monitoring of conditions (e.g., through machine-learning methods) to detect potential threats.

6. **Promote a proactive culture:** Organizations should provide incentives for early-bird alerts on anomalous operating conditions, which promote flexibility and a proactive response in the face of an unforeseen threat.

About the Authors

Omera Khan is a Full Professor of Operations Management at the Technical University of Denmark. She works with leading organizations on a range of supply chain and logistics issues and is advisor to many universities developing courses in logistics, supply chains, and operations management. She has led and conducted research projects commissioned by government agencies, research councils, and companies in supply chain resilience, responsiveness, sustainability, and the impact of product design on the supply chain. Her latest area of research focuses on cyber-risk and resilience in the supply chain. Omera is an advisor to many organizations and provides specialist consultancy in supply chain risk management. She is a highly acclaimed presenter and is regularly invited as a keynote speaker at global conferences and corporate events. She has published her research in leading journals, contributed to several book chapters, and is lead author of *Handbook for Supply Chain Risk Management: Case Studies, Effective Practices and Emerging Trends*. She founded and was Chair of the Supply Chain Risk and Resilience Research Club and the Product Design and Supply Chain Special Interest Group. She has also been a visiting professor at a number of leading business schools.

Daniel A. Sepulveda Estay is a PhD researcher at the Technical University of Denmark, where he researches cyber-risk and security in the global supply chain. He has worked in the engineering and supply divisions of a number of multinational companies, both in strategic/leadership and operational roles for over 11 years, having partially led initiatives such as the implementation of lean manufacturing in Coca-Cola Company Latin America and supply rationalization in BHP Billiton´s copper projects division. Daniel has a BSc in Mechanical Engineering from the Federico Santa Maria Technical University in Valparaiso, Chile, an MSc degree in Industrial Engineering from the Pontifical Catholic University of Chile in Santiago, Chile, and an MSc degree in Management from the MIT Sloan School of Management, in Boston, United States.

Supply Chain Cyber-Resilience: Creating an Agenda for Future Research

Omera Khan and Daniel A. Sepúlveda Estay

References

Asbjornslett, B. E. 1999. Assess the Vulnerability of Your Production System. *Production Planning & Control,* 10(3): 219–229. http://dx.doi.org/10.1080/095372899233181

Bailey, T., Miglio, A. Del, & Richter, W. 2014. The Rising Strategic Risks of Cyberattacks. *McKinsey Quarterly,* 2 (2014): 17–22.

Blackhurst, J., Dunn, K. S., & Craighead, C. W. 2011. An Empirically Derived Framework of Global Supply Resiliency. *Journal of Business Logistics,* 32(4): 374–391. http://dx.doi.org/10.1111/j.0000-0000.2011.01032.x

Boyson, S. 2014. Cyber Supply Chain Risk Management: Revolutionizing the Strategic Control of Critical IT Systems. *Technovation,* 34(7): 342–353. http://dx.doi.org/10.1016/j.technovation.2014.02.001

BSI. 2008. *BS ISO/IEC 27001:2008 Information Technology – Security Techniques – Information Security Risk Management.* London: British Standards Institution.

Burnson, P. 2013. Supply Chain Cybersecurity: A Team Effort. *Supply Chain Management Review,* June (2013): 6–8.

Christopher, M., & Peck, H. 2004. Building the Resilient Supply Chain. *International Journal of Logistics Management,* 15(2): 1–14. http://dx.doi.org/10.1108/09574090410700275

Christopher, M., & Towill, D. 2001. An Integrated Model for the Design of Agile Supply Chains. *International Journal of Physical Distribution & Logistics Management,* 31(4): 235–246. http://dx.doi.org/10.1108/09600030110394914

Deloitte. 2012. *Aftershock: Adjusting to the New World of Risk Management.* London: Deloitte Development LLC.

Deloitte. 2013. *The Ripple Effect: How Manufacturing and Retail Executives View the Growing Challenge of Supply Chain Risk.* London: Deloitte Development LLC.

ENISA, 2015. National Cyber Security Strategies in the World. *European Union Agency for Network and Information Security.* Accessed April 1, 2015: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world

Gerencser, M., Weinberg, J., & Vincent, D. 2003. *Port Security War Game: Implications for U.S. Supply Chains.* Booz & Company.

German Federal Ministry of the Interior. 2005. *National Plan for Information Infrastructure Protection.* Berlin: Bundesministerium des Innern.

Intel Security. 2014. *Net Losses: Estimating the Global Cost of Cybercrime.* Santa Clara, CA: Intel Security

IRM. 2015. Cyber Risk and Management. *Institute for Risk Management.* Accessed April 1, 2015: https://www.theirm.org/knowledge-and-resources/thought-leadership/cyber-risk/

Keegan, C. 2014. Cyber Security in the Supply Chain: A Perspective from the Insurance Industry. *Technovation,* 34(7): 380–381. http://dx.doi.org/10.1016/j.technovation.2014.02.002

Linkov, I., Eisenberg, D. A., Bates, M. E., Chang, D., Convertino, M., Allen, J. H., Flynn, S. E., & Seager, T. P. 2013. Measurable Resilience for Actionable Policy. *Environmental Science and Technology,* 47(18): 10108–10110. http://dx.doi.org/10.1021/es403443n

Pettit, T. J., Fiksel, J., & Croxton, K. L. 2010. Ensuring Supply Chain Resilience: Development of a Conceptual Framework. *Journal of Business Logistics,* 31(1): 1–21. http://dx.doi.org/10.1002/j.2158-1592.2010.tb00125.x

Ponemon. 2014. 2014 *Global Report on the Cost of Cyber Crime.* Traverse City, MI: Penemon Institute.

Reuters. 2012. *Cyber Crime - How Can Firms Tackle This Fast-Emerging Invisible Menace?* London: Thomson Reuters.

Sheffi, Y., & Rice, J. B. 2005. A Supply Chain View of the Resilient Enterprise. *MIT Sloan Management Review,* 47(1): 41–48.

Tranfield, D., Denyer, D., & Smart, P. 2003. Towards a Methodology for Developing Evidence-Informed Management Knowledge by Means of Systematic Review. *British Journal of Management,* 14(3): 207–222. http://dx.doi.org/10.1111/1467-8551.00375

WEF. 2012. *Risk and Responsibility in a Hyperconnected World - Pathways to Global Cyber Resilience.* Geneva, Switzerland: World Economic Forum.

WEF. 2013. *Building Resilience in Supply Chains.* Geneva, Switzerland: World Economic Forum.

WEF. 2015. *Partnering for Cyber Resilience: Towards the Quantification of Cyber Threats.* Geneva, Switzerland: World Economic Forum.

White House. 1998. *Presidential Decision Directive NSC-63 on Critical Infrastructure Protection.* Washington, DC: The White House.

White House, 2003. *The National Strategy to Secure Cyberspace.* Washington, DC: The White House.

Citation: Khan, O., & Sepúlveda Estay, D. A. 2015. Supply Chain Cyber-Resilience: Creating an Agenda for Future Research. *Technology Innovation Management Review*, 5(4): 6–12. http://timreview.ca/article/885

Keywords: resilience, supply chain management, cyber-risk, cybersecurity, theoretical foundation